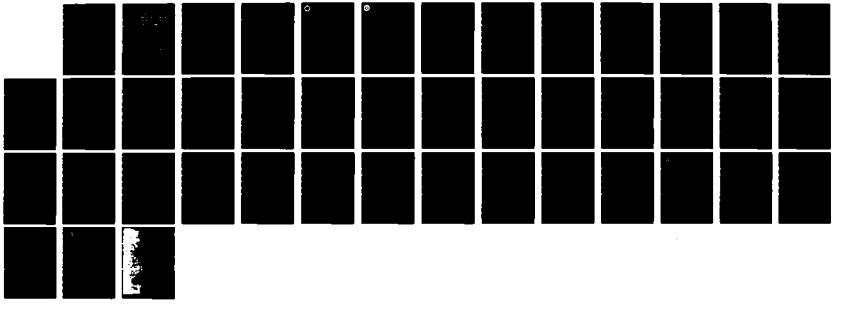
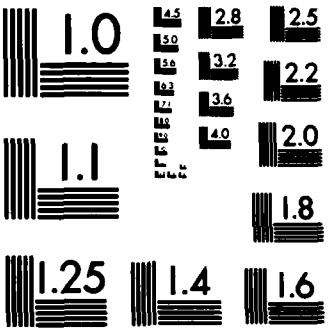
AD-A127 476 REPORT OF DEFENSE SCIENCE BOARD TASK FORCE ON AUTODIN II(U) OFFICE OF THE UNDER SECRETARY OF DEFENSE FOR RESEARCH AND ENGINEERING WASHINGTON DC DEC 82 1/1

UNCLASSIFIED F/G 17/2 NL





(2)

REPORT OF DEFENSE SCIENCE BOARD TASK FORCE ON AUTODIN II

DECEMBER 1982

OFFICE OF
THE UNDER SECRETARY OF DEFENSE
FOR RESEARCH & ENGINEERING
WASHINGTON, DC

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

REPORT DOCUMENTATION PAGE		READ INSTRUCTIONS BEFORE COMPLETING FORM
1. REPORT NUMBER	2. GOVT ACCESSION NO. AD-A127476	3. RECIPIENT'S CATALOG NUMBER
4. TITLE (and Subtitle) Report of Defense Science Board Task Force on AUTODIN II		5. TYPE OF REPORT & PERIOD COVERED
		6. PERFORMING ORG. REPORT NUMBER NA
7. AUTHOR(s) NA		8. CONTRACT OR GRANT NUMBER(s) NA
9. PERFORMING ORGANIZATION NAME AND ADDRESS Defense Science Board, OUSDRE Room 3D1020, The Pentagon Washington, D.C. 20301		10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS NA
11. CONTROLLING OFFICE NAME AND ADDRESS Same as Above		12. REPORT DATE December 1982
		13. NUMBER OF PAGES 43
14. MONITORING AGENCY NAME & ADDRESS (if different from Controlling Office) Same as Above		15. SECURITY CLASS. (of this report) UNCLASSIFIED
		15a. DECLASSIFICATION DOWNGRADING SCHEDULE

16. DISTRIBUTION STATEMENT (of this Report)

Cleared for Open Publication

DISTRIBUTION STATEMENT A
Approved for public release
Distribution Unlimited

17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)

18. SUPPLEMENTARY NOTES

19. KEY WORDS (Continue on reverse side if necessary and identify by block number)

20. ABSTRACT (Continue on reverse side if necessary and identify by block number)

DD FORM 1 JAN 73 1473 EDITION OF 1 NOV 65 IS OBSOLETE

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

REPORT of DEFENSE SCIENCE BOARD TASK FORCE

on

AUTODIN II

December 1982

Office of the Under Secretary of Defense for Research & Engineering

Washington, D.C.

OFFICE OF THE SECRETARY OF DEFENSE
WASHINGTON, D.C. 20301

DEFENSE SCIENCE BOARD

9 February 1983

MEMORANDUM FOR SECRETARY OF DEFENSE
CHAIRMAN, JOINT CHIEFS OF STAFF

THROUGH: UNDER SECRETARY OF DEFENSE FOR RESEARCH AND ENGINEERING

SUBJECT: Final Report of the DSB Task Force on AUTODIN II

I am pleased to forward the final report of the DSB AUTODIN II Task Force. Consistent with the Task Force's recommendation, the AUTODIN II approach to a common user data network was cancelled by the Deputy Secetary of Defense on 2 April 1982. The recommended alternative Defense Data Network (DDN), an evolutionary approach, was started at the same time. In making their recommendation, the Task Force identified several areas in the new program which may require special attention. In particular, it will take a diligent effort from central management in the OSD to control the tendency of users to develop separate dedicated data networks rather than join the common user net. Moreover, some questions about the role of the National Security Agency in the certification of the new system were surfaced.

The Task Force's most important finding is that the establishment and maintainence of a common user data network should remain DoD policy. This was also reaffirmed in the Deputy Secretary of Defense memorandum of 2 April 1982. Dr. Stevens, the Task Force Chairman, recommended that continued high level review would be extremely valuable to the effective implementation of such a network. By separate correspondence I am recommending to Dick DeLauer that he consider assigning this new undertaking to Dr. Steven's Task Force under an updated charter.

This report has been approved by the Defense Science Board and I recommend that you read Dr. Steven's cover letter and the two page executive summary.

Norman R. Augustine
Chairman

Attachment

Copy to:
Director, DCA

OFFICE OF THE SECRETARY OF DEFENSE
WASHINGTON, D.C. 20301

DEFENSE SCIENCE BOARD

December 30, 1982

MEMORANDUM FOR THE CHAIRMAN, DEFENSE SCIENCE BOARD

SUBJECT: Final Report of the Task Force on AUTODIN II

On behalf of my Task Force members, I am pleased to submit herewith our final report on the AUTODIN II data communications network. In developing our recommendations with regard to the termination of this program, the Task Force met for six formal sessions and various members met on many other occasions to discuss the issues or to hear from involved Agencies. Our conclusions and recommendations can be found, in abbreviated form, in the Executive Summary. The recommendations were acted upon in April 1982 by the Deputy Secretary of Defense. We further met in October 1982 to review the progress of the implementation of the alternative data communication network which we had recommended as the better approach. Some concerns with the role of the National Security Agency in the certification of the system as being free of denial of service problems are noted in the epilog to our report. However, with this exception the progress in developing the Defense Data Network made since the AUTODIN II termination decision is encouraging. We see no insurmountable hurdles in the way of the DDN.

The unstinting cooperation received from all concerned is most noteworthy. In particular, the DCA evaluation effort was well done under circumstances of high institutional stress. We are indebted to all those who assisted us in this task.

Although we have executed the letter of our charter by the production of this report, I feel that there would be significant value in the occasional reconvening of this Task Force to review, as we did in October, the progress of the evolution of the Defense Data Network.

Sayre Stevens

Sayre Stevens
Chairman
Task Force on AUTODIN II

Attachment

CONTENTS

EXECUTIVE SUMMARY

In September 1981, the Defense Science Board was requested to evaluate the AUTODIN II data communications system in relation to presently available alternatives and to make recommendations concerning the continuation or termination of that partially operational system. The Task Force reviewed the Defense Communications Agency's evaluation of a revised AUTODIN II system and an alternative based upon ARPA Network technology. It further reviewed the proposed new systems themselves on the basis of technology, survivability, security, and cost. The Task Force's final preference for the evolutionary ARPA Network approach was in agreement with DCA's conclusion that it was the better of the two, and was reached without regard to AUTODIN II programmatic deficiencies.

The findings and recommendations of the Task Force follow:

1. OSD should reaffirm the need for a common-user network.

2. Make a choice between AUTODIN II and the ARPA Network approach promptly; our review favors the selection of ARPA Network.

We doubt that the preservation of AUTODIN II will significantly further the achievement of a common user net. Moreover, we believe that a better technical foundation for a Defense Data Network (DDN) is available. Though there are some significant programmatic and management risks associated with relying on accretions to the ARPA Network Foundation, we believe that these involve the extent and pace of common user participation and not risks involved in achievement of a common user net.

The most immediate impact of terminating AUTODIN II will be felt by users operating at the Secret level who might have been served more quickly by that system than by additions to the ARPA Network base. While the User Requirements Data Base (URDB) does not include a large number of Secret users, it is unquestionably incomplete.

3. In pursuing the development of DDN, follow a program of gradual expansion of the ARPA Net-compatible base with an eye toward the ultimate interconnection of individual nets.

But, this can only be done through aggressive pursuit of a fully developed program for the establishment of a broad common user network by institutionalized management and if the accretive process occurs under stringent configuration control.

4. The solution to the multi-level security problem for an ARPA Net System requires the development of new security safeguard concepts like BLACKER. The IPLI is an interim solution that is suitable until multi-level secure hosts become available.

The current IPLI program should be strengthened and the development consortium of DCA, DARPA, and NSA replaced by a single program manager. BLACKER development should be given higher priority.

On April 2, 1982, the Deputy Secretary of Defense directed the termination of AUTODIN II and implementation of the alternative proposal.

DISCUSSION

I. THE PROBLEM

The growth in defense data systems and the need for associated communications increasingly urge the development of a common user network serving a wide range of needs. The advantages of having such a network are substantial and manifold. The possibilities for interoperability are significant. At the outset of the Task Force's deliberations, representatives of the JCS had identified as many as 58 separate systems requiring a capacity for interoperability. The common use of a richer, more complex network can allow better reliability, greater surge capacity and some cost advantages over dedicated links. To implement such a system poses some severe problems, however. Not the least of these is a requirement for multi-level security, that is, service of users trafficking in information of substantially different levels of classification.

AUTODIN II was undertaken in 1976 after the consideration of alternative approaches by DoD Data Internet Study in 1975. AUTODIN II was designed as a packet-switch network relying upon a security kernel to provide the multi-level security required for the system. The kernel was to consist of software in which trust had been acquired through extensive test and validation and protection from outside access. Because end-to-end encryption was not included in the system architecture, information within the switches was in the clear requiring large, manned, and highly secure facilities. One result was a system topology consisting of relatively few network nodes.

As a two year program stretched to four and a half years, a growing number of problems and uncertainties about AUTODIN II were encountered. In July 1980, an OSD review group was established to review the system. With the assistance of DCA, the group considered the cost, security, performance, and survivability of AUTODIN II. Because for a considerable time it appeared that the system might not achieve IOC, the group also explored available options if AUTODIN II failed. Principal among the alternatives considered was expansion of the WWMCCS Information Network (WIN) and ARPANET systems. AUTODIN II did achieve a partial IOC in July 1981, though testing on some major components was forced to continue.

Major concerns about the system remained. Because it comprised only four nodes -- it was planned that it would grow to eight -- survivability of the system was extremely limited. It must be noted that at the inception of the program, survivability was not a major, explicit requirement. But as greater emphasis was put on C^3I survivability, the design of AUTODIN II made its achievement through expansion and the proliferation of nodes an unattractive option.

Time delays were producing scheduling difficulties and eroding user acceptance of a system that was continually promised but never really ready for use. Because the creation of a common user network requires weaning users away from the use of dedicated links entirely under their own control, the advantages of moving to a common-user system have to be very attractive. Continuing delays served to reinforce natural preferences for dedicated links.

Projected costs continued to grow as a result of increasing backbone tariff charges and the costs of the relatively long access lines necessitated by the small number of AUTODIN II switches. Studies of comparative costs showed large disadvantages relative to dedicated system costs further reducing user acceptance of AUTODIN II.

Continuing difficulties had been encountered with the security kernel and its acceptance as sufficiently trustworthy to allow certification of the system to handle traffic beyond the Secret level of classification. Problems of interpreting the meaning of security requirements associated with the format and documentation of kernel software had produced significant additional costs to the government and were responsible for much of the slip in schedule. Despite efforts to go back and re-do some of the work, NSA's recommendations continued to call for constraints on system operation with classified users. Moreover, it appeared likely that acceptance for the use of special intelligence traffic would require the addition of end-to-end encryption, a step originally believed to be unnecessary by the use of the multi-level security kernel approach.

Finally, limitations on the testing that had been performed on AUTODIN II left plaguing uncertainties as to whether or not system performance would be adequate despite its having achieved partial IOC.

In these circumstances OUSDR&E (C^3I) urged that alternatives to AUTODIN II be seriously considered; this led to the fleshing out of an optional approach by DCA based on an implementation of heavily tested WIN/ARPANET technology. In August 1981, DCA agreed to conduct a formal, comparative evaluation of AUTODIN II and its alternative.

The DSB AUTODIN II Task Force was formed to provide an appraisal of the situation by an objective outside group that was a priori committed to neither alternative. The charge to the Task Force was simple and direct. It stressed an early response to the problem.

The Defense Science Board Charge

- Review, evaluate, and make recommendations concerning the continuation/termination of DCA AUTODIN II data communications system.
- Address questions of survivability, cost and security for AUTODIN II and presently available alternatives.
- Review ongoing evaluation of both alternatives currently being conducted by DCA.
- Final report no later than February 15 with interim reports as issues are resolved.

The Task Force was established in late September 1981 and members were selected and approved by December.

AUTODIN II Task Force Membership

Van Doubleday	Honeywell Information Systems
Seymour Goodman	University of Arizona
Gerald Popek	UCLA
Harold Rosenbaum	HRA, Inc.
John Stenbit	TRW Systems Group
Sayre Stevens	System Planning Corporation, Chairman
Willis Ware	Rand Corporation
Stephen Walker	ODUSD(C^3I), Exec. Secretary
LCdr Ralph Chatham	DSB, DSB Point of contact

The meeting schedule was tied to the DCA comparative evaluation timelines and members met in Washington on January 21-22, February 18-19, and March 4-5, 1982. The original schedule was extended as DCA found that more time was required to carry out a detailed and interactive evaluation of the two data network plans.

The Task Force submitted its recommendations to the Chairman of the DSB on March 8 and, because of the urgency of this issue, forwarded them to the DUSDR&E (C^3I) the following day with the caution that they had not been approved by the full Board. Results of the study were briefed to the DUSDR&E (C^3I) and the Director of DCA on March 9 and to USDR&E on March 12. In each case, note was taken of the fact that Board approval had not yet been obtained though its Chairman had reviewed the briefing in chart form. On May 5, the entire DSB was briefed on the results of the Task Force's review of AUTODIN II and an alternative based on the WIN/ARPANET implementation of packet-switching technology. The Board raised no objection to issuance of the findings of the Task Force.

II. DCA ALTERNATIVES EVALUATION

Against this background, the Task Force undertook to look first at the DCA Alternatives Evaluation. It considered the methods used by DCA in evaluating two different approaches to meeting the computer communications network needs of the Defense Department and then at the specific conclusions it reached. The Task Force then made its own evaluation of the two alternatives and finally produced a number of recommendations as to the approach that it felt should be taken by OSD and DCA given the circumstances that obtained.

DCA Alternatives Evaluation

- o Competitive Process
  - Two design teams with contractor support
  - Defined requirements
  - Non-disclosure
  - Short time with limited interaction with evaluators
  - Good performance
- o Evaluation Process
  - Separate team
  - Well established criteria emulating contractor selection
  - Complex quantitative method based on disaggregated subjective judgments
  - Care given to avoidance of bias
  - Taken seriously - A major effort

Competitive Design Process

The DCA evaluation process was based upon a competitive design effort. Two teams were established; one supporting the further development of AUTODIN II and the other supporting the development of a new packet-switching approach based upon ARPANET experience and the expansion of the WIN/ARPANET base that already existed. The use of two design teams to prepare what were essentially proposals served to force a binary decision in the evaluation. Thus, the selection was made between one of the two approaches rather than an attempt to find a solution to the problem which was in some sense optimized. It must also be noted that the proposals that were produced and were evaluated differed substantially from AUTODIN II as it had been originally designed and as it currently existed and from the basic ARPANET system. New designs, new technologies, and new approaches were incorporated in both of the proposals. The ARPANET approach was given the name of the REPLICA system.

This competitive approach benefitted by producing an evaluation of two approaches that had been improved and tuned to the needs as they were felt by DCA and the user community at the time the evaluation took place. It also had some drawbacks, however, as it limited the review to the specific characteristics of the two designs. The evaluation consisted of the two design teams, an independent evaluation team, and substantial analytical support that was provided to both teams. This supporting effort produced, at the outset of the evaluation process, a set of requirements that both designs were to meet. These requirements also included the establishment of a User Requirements Data Base (URDB) which defined the number of users to be expected and their specific requirements. As suspected at the time by DCA, the URDB proved later to have been incomplete and to have revealed less than the full range of user requirements that is likely to emerge in the years ahead. But nevertheless, both teams were presented with the same requirements so that a uniform basis for evaluation was established. Contractor support was provided to both teams which included the prime contractors for the AUTODIN II and ARPANET systems. Both contractors contributed substantially to the design and, in effect, made design proposals and cost estimates. Strong ground rules were established with regard to non-disclosure between members of the team and those participating in the process so that the evaluation was run in a fairly well defined and disciplined fashion. The Task Force was not in a position to determine, nor did it try to determine, how faithfully these rules were observed by the various participants in the process.

It was our conclusion, however, that both teams did a good job, produced credible proposals worthy of serious consideration and that the process did indeed move the development of a defense data network substantially beyond the point it had been before the evaluation took place. It must also be remembered that this evaluation process took place in a very short period of time and with a limited amount of interaction among all of those participating. One might argue that more interaction and a looser, more generally innovative approach might have produced better designs. Under the circumstance, however, the Task Force concluded that the approach was probably a good one and that it was a useful undertaking.

Evaluation Process

With the completion of the designs by the two teams, they were turned over to the evaluation team which played a totally independent role. The evaluation team reviewed both proposals, considered them against pre-established criteria as to value, and considered the ability of both systems to meet established requirements. The evaluation team comments were fed back to the two design teams who then had an opportunity to make improvements and changes to their proposals to meet shortcomings that were identified. The two proposals were then reviewed and were quantitatively scored and a final judgment made as to which of the two approaches appeared to be the better.

The evaluation team's determination was undertaken on the basis of a complex quantitative method which relied in the end on highly disaggregated judgments. There is little else that could have been done. They used, as noted above, well established criteria in a fashion that attempted to emulate a stiff, controlled contractor selection process. Clearly the efforts of the evaluation team were taken seriously and it constituted a major effort on the part of DCA to work through this process. Care was given to the avoidance of bias and indeed there was every indication that extreme steps were taken to insure that this was the case. The final conclusion of the evaluation panel was given on February 25, 1982, and was approved by the Director of DCA the following day.

Conclusion of DCA Evaluation

"REPLICA Approach Provides the Best (SIC) DoD Data Network"

The Task Force spent some time reviewing the judgments and the methods used by the evaluation team in reaching this result.

Task Force Appraisal of DCA Evaluation

- o Reached without regard to AUTODIN II difficulties
- o Noted nearly all of the WIN/ARPANET technology approach advantages identified by the Task Force
- o Perceptively noted several concerns
  - Contractor promises without commitments
  - Shortcomings of either/or decision
  - Risks
- o Conscious of importance of user satisfaction
- o Some uneven treatment
- o Carefully unbiased
- o Job well done in circumstances of high institutional stress
- o Outstanding support for DSB Task Force

DCA Conclusion

It is a strength of the evaluation that the decision was reached by the evaluation panel largely without regard to AUTODIN II programmatic difficulties. This fact is important because the problems of AUTODIN II had become contentious by this stage and there were substantially differing appreciations of the state of the AUTODIN II system at the time the evaluation took place. The Task Force had difficulty in determining the true state of affairs with regard to AUTODIN II because of these conflicting reports. Thus, the conclusions reached are strengthened by the fact that the decision in favor of the WIN/ARPANET approach did not rely upon one or another of these evaluations of the difficulties that AUTODIN II was or was not encountering. A possible exception to this in the evaluation team's appraisal exists in the management overview section which noted the difficulties that Western Union had in bringing AUTODIN II on line. Nevertheless, this was not a major factor in the evaluation.

Features of DCA Evaluation

The Task Force found that the DCA evaluation had noted almost all of the technical advantages of the ARPANET approach which the panel itself had identified. Moreover, it noted a number of concerns quite perceptively. This is particularly significant because they were the types of concerns that might have been missed in the process as it was established. It noted, for example, that both proposals relied in their design upon contractor promises without an actual commitment to deliver for the costs and on the schedules that were included in the proposals. The shortcomings of making an either/or decision rather than finding some third ground in designing a new approach to the system were also recognized. A number of significant risks and concerns were noted. The performance of both systems was dependent upon their ability to operate with a significant increase in the number of nodes in the system topology, and consequently, remained uncertain. The ARPANET hardware development question was noted. Particularly the problems associated with the rapid production of a large number of C-30 switches was seen as a risk that had to be taken into account. In that regard, the capacity of BB&N as a relatively small firm to fulfill the prime contract responsibilities that seemed incumbent upon it with the selection of ARPANET approach were recognized. Questions were raised as well about Western Union management performance as it had dealt with AUTODIN II to date. Inadequacies in the URDB were noted and a good deal of skepticism of its realism displayed in the evaluation.

In its deliberations, the evaluation team showed consciousness of the importance of user satisfaction in system design, but really was forced to deal with it in general terms, and did not come to grips with many of the specific impacts that the move to common user networks are apt to have on individual users. These considerations are particularly important when one is dealing with the relatively small, lower priority, unclassified user who must in the end pay for a substantial number of features that are important only to the higher priority classified users when they join a common user network. In the evaluation, we found some uneven treatment. Survivability treatment was fairly good though limited. The treatment of security also appeared to be given limited consideration and we felt there were significantly more important factors relative to security to be taken into account.

From the results of the evaluation it appeared that the process had been undertaken in a carefully unbiased way. All in all, the Task Force concluded that the evaluation was well done in difficult circumstances. Certainly, the evaluation and the entire process involved put high institutional stress on DCA. It was clear that feelings ran high, that competition was severe and that many people felt that their professional stature was at risk in the evaluation. The support given to the Task Force by both design teams and by the evaluation team and by the leadership of DCA was outstanding throughout the period of its review. No question was asked for which an answer wasn't provided and, quite beyond that, substantial amounts of material were made available to the Task Force for its use.

III. DSB TASK FORCE EVALUATION

What follows is the Task Force's own evaluation of the two alternatives. This evaluation is based upon a consideration of design and technology factors, survivability considerations, security considerations, cost, user satisfaction, and the outlook for the development of a common user network. It concludes with the delineation of some major concerns that were identified in the evaluation process.

John Stenbit wishes to note that the Task Force Evaluation as presented here tends to focus on considerationns it felt supported the choice of the ARPANET approach, and consequently masks a substantially less obvious choice between the two systems. While he does not take issue with the choice made, he feels that the presentation does not represent the full range of considerations involved. He believes that what follows has greater utility as guidance to proceeding with the implementation of an ARPANET decision than in providing the basis for making such a decision.

The Task Force Evaluation of the Alternatives

- o Design and technology favor WIN/ARPANET implementation technology.
  - Maturity of technology
  - State-of-the-art
  - Evolutionary potential
  - Security approach
  - Manpower
  - Interconnection issues

Design and Technology

Maturing of Technology

As a result of the evaluation, the Task Force found that design and technology considerations strongly favored the ARPANET/WIN approach as a basis for the development of a computer communications network. It found these advantages to be more substantial than the DCA evaluation suggested that they were. Principal among them was the maturity of the technology involved. The operational use of ARPANET, WIN, COINS, PLATFORM has given the defense community many years experience with the technology involved. Moreover, experience with these systems involves operation with quite a large number of nodes in the case of ARPANET, but certainly with more nodes in all cases than has been possible with the limited operational capability of AUTODIN II. The extensive upgrading of the ARPANET software over the years is another important feature of system maturity. This software is heavily tested and has undergone a long period of evolution and improvement to its reliability and efficiency that has carried it well beyond its initial state.

State of the Art

At the same time, the Task Force concluded that this maturity came without the costs of outmoded technology. Though the technologies embodied in the ARPANET approach are more mature than those of AUTODIN II, the state of the art of the technology embodied in the REPLICA proposal is substantially more advanced than that of the ARPANET system. Certainly the BB&N C-30 computer is a step ahead of the PDP-11 used in AUTODIN II. The topology of the REPLICA system is substantially more sophisticated than that of AUTODIN II and the routing algorithm used in the ARPANET system is substantially stronger than that developed for AUTODIN II.

Evolutionary Potential

A third consideration involved the evolutionary potential of the two systems. The Task Force believes that the evolutionary potential of the ARPANET approach was substantially greater than that of AUTODIN II. One consideration in this regard is the fact that AUTODIN II is a leased system whereas, the ARPANET is and the proposed REPLICA will be owned by the government. Difficulties encountered in instituting changes in any leased system not owned by the government argue in favor of avoiding the leasing approach in an evolutionary system. Moreover, a large experimental test bed exists in the ARPANET system which has allowed the use of the network in communications that involve a significant throughput of material by a large number of users employing a wide range of user operations. This is a better base on which to build than is provided by AUTODIN II.

Security

The Task Force favored the security approach involved in the REPLICA proposal over that of AUTODIN II. Difficulties with the security kernel approach, which is the essence of the AUTODIN II design, proved to be substantial; similar experience has been found with far less ambitious kernel designs. The problem is largely derived from difficulties encountered in endeavoring to verify the integrity of the software employed. It must be done in a rigorous and formalistic fashion that will allow absolute trust to be established that all instructions have intended effects and that no malicious instructions are concealed in the code. The immaturity of the kernel technology and the large size of the AUTODIN II kernel combined to greatly amplify these verification problems. The kernel approach is further complicated by requirements for recertification after each software change. This proved in fact to be a problem with AUTODIN II. The kernel also has unpleasant operational effects because it is specifically designed to be inaccessible from outside. Thus, those working with the system are denied the opportunity of making internal measurements in the process of debugging the system. Moreover, modifications that involve kernel software cannot be accomplished because of its inaccessability. This situation occurred in the DCA redesign of AUTODIN II for the evaluation when the number of precedence levels could not be increased because of kernel limitations.

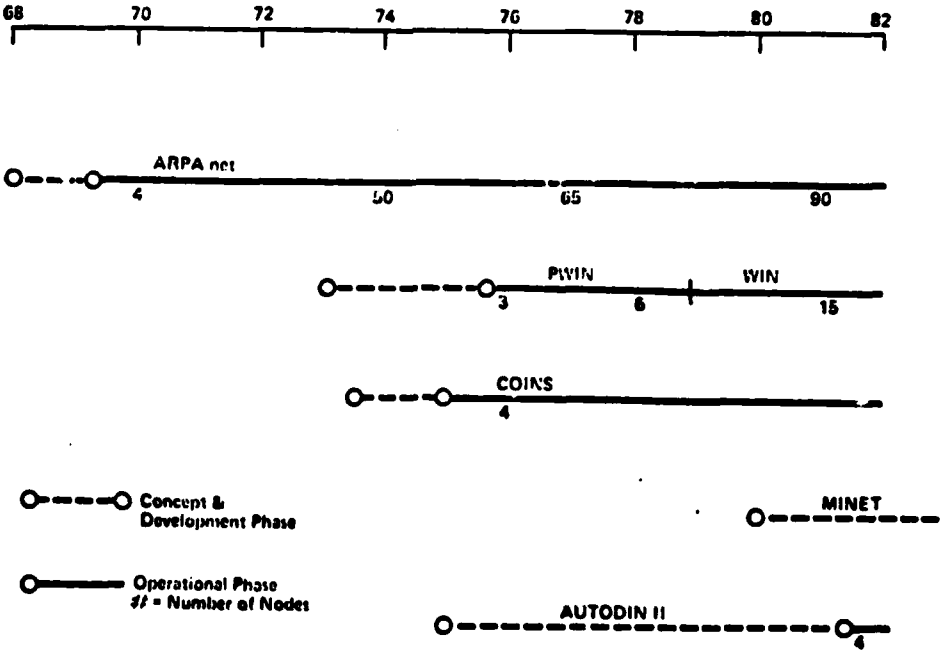
End-to-end encryption, on the other hand, tends to decouple security from almost all other issues and this is the approach taken in the ARPANET design. There are, however, problems associated with it, including the replication of cryptographic hardware, and it is important to note that the achievement of true multi-level security depends on the availability of both hardware and trusted software not yet available. Full achievement of multi-level security for the proposed REPLICA system thus requires the availability of BLACKER, an interface device incorporating electronic key distribution being developed by NSA, and the development of trusted multi-level host computer systems.

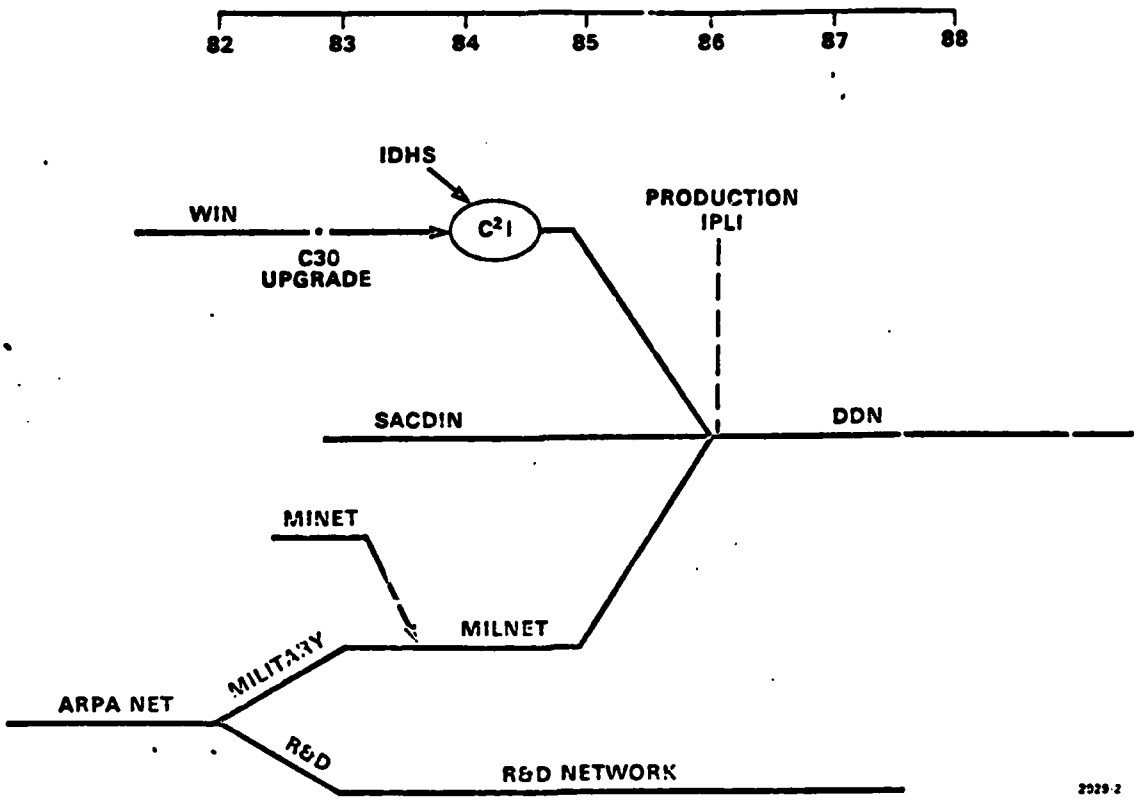
Manpower

Insofar as manpower is concerned, and this is an important consideration, the REPLICA system has a clear advantage by having unmanned switches located in secure facilities where part-time maintenance is available when required.

Interconnection Issues

A number of interconnection issues favor the ARPANET/WIN approach as well. The incremental network growth favored by the Task Force is clearly more compatible with the ARPANET design. There are more nodes with shorter access lines. Smaller increments in growth occur as new networks are added and there is a standing set of networks already existing which can be pulled together to form ultimately a true common user network operating at all security levels. The advantages of such incremental network growth are strengthened as well by the upgrades that are currently planned for both WIN and the intelligence net, IDHS, which will make them compatible with other candidates for ultimate consolidation. The evolutionary time-table is shown in the following figures.





Interconnection advantages are also amplified by the extensive host interface development that has already successfully been accomplished by ARPANET. There have been many, many host interfaces built for a wide range of computer systems so that a step ahead has been taken in dealing with this difficult problem. The substantial amount of university training that has occurred with ARPANET also acts in this regard.

Survivability

- o Survivability considerations are ill-defined but seem to favor WIN/ARPANET.
  - Lack of agreed survivability criteria makes objective appraisal difficult - needs to be addressed.
  - Nature of Soviet threat makes proposed nodal proliferation almost trivial in nuclear attack.
  - It is more significant to survivability against conventional attack and important in the case of sabotage, however.
  - Greater suitability of WIN/ARPANET nodes for mobile, unmanned, deceptive deployment may be even more important.

Problems in Analyzing Survivability

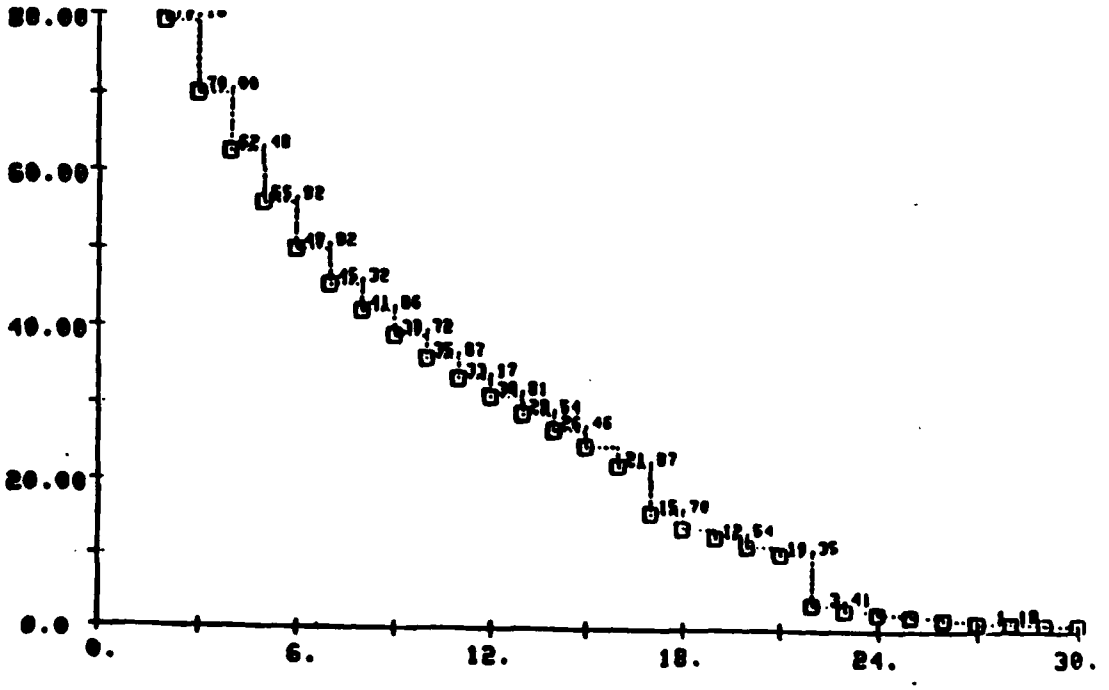
The Task Force had difficulty in dealing with the issue of survivability. This difficulty was based upon the impossibility of talking meaningfully about the survivability of a broad communications system within the U.S. in the face of nuclear attack. There simply are not adequate, agreed criteria to use in dealing with that question. Moreover, the uneveness in vulnerability of the various elements of such communications systems undermines the apparent value of hardening individual elements while others remain soft. The elements of a survivability program that are focused upon the gradual development of survivability with accretions to our communications system over time seem to be lacking. Importance must be given to steps which if taken now may not provide immediate survivability but will be compatible with the future achievement of substantially higher levels of survivability, as new equipment replaces old and new designs are adopted.

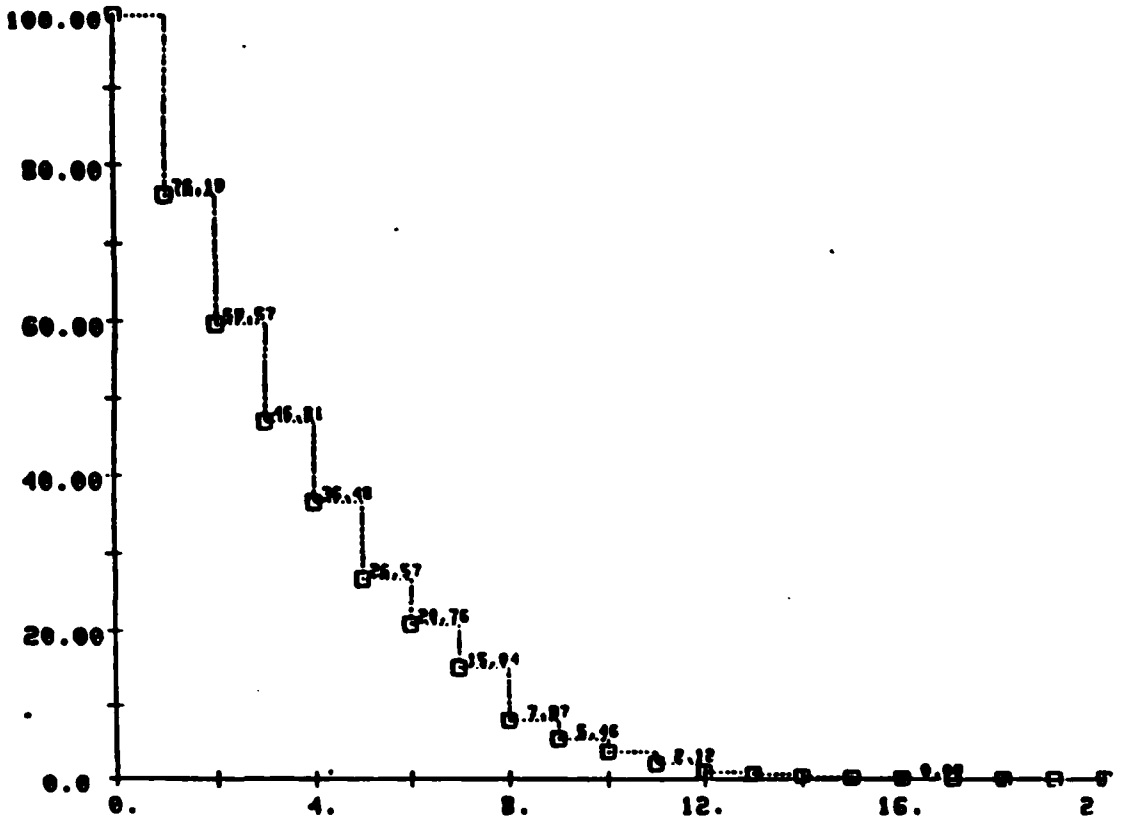
Two approaches were continually brought up in our discussions with DCA and OSD on the subject of C^3 survivability. One was a well established policy of DCA to avoid collateral damage by locating communications elements in areas where they will not be lost as byproducts of attacks on other major military targets. Soviet belief in the importance of early attacks on command and control facilities clearly indicates that collateral damage avoidance is an inadequate approach to achieving survivability. Significant communications nodes are important targets to the Soviets and almost certainly would be included in their targeting plans. They have plenty of available weapons to use in such planning. The other approach encountered was simply one of writing off the need for links as the destruction of the user facilities occurs during attack. This approach argues that if a base is lost there really is no requirement remaining for it to communicate over the data network; there is an underlying assumption, however, that its loss will not impair the performance of the rest of the network. This view of the problem seems to us to have failed to deal adequately with the matter of reconstitution and with the possibility in the future of force dispersal.

Survivability in the Face of the Soviet Threat

The problem is made worse by the fact that the current estimates of Soviet weapons inventory growth make the costs associated with attacking either of the proposed data network systems almost trivial in terms of the amount of node proliferation that is included in either design. When coupled with the importance given by the Soviets to disrupting command and control in the early phases of the war, evading Soviet attack through simple proliferation at the levels talked about in these designs is not going to be a successful approach. On the other hand, the levels proposed do have some significance in terms of survivability against conventional attack and are important in the case of sabotage.

The DCA evaluation of comparative survivability was made within a narrow range of considerations focusing on a measure of the graceful degradation of the two systems under varying levels of attack. Because it has more nodes, the ARPANET approach obviously fared better in this analysis. In either case, however, survivability in the face of a serious attack was limited. In the case of ARPANET, an optimized nuclear attack on 20 nodes would reduce system connectivity to about ten percent. Comparable effects occurred in the AUTODIN II system with the loss of eight nodes. The figures below show these effects.





Growth Toward Survivability

In the end, the Task Force chose to pay particular attention to the suitability of the two systems to meet the demands of a policy of growth toward survivability that requires that a start be made now even without balanced survivability across the entire network. From this vantage point, the ARPANET approach seems to have some significant advantages. It is far more suitable for mobile, deceptive and unmanned deployment which may in the long run prove to be important ingredients in the development of more robust and genuinely survivable communications systems. Thus, the Task Force gave the nod to ARPANET in this regard.

Security

The Task Force found the review of security considerations to be similarly frustrating. It identified several factors which badly complicated the process of certifying the use of any system for the communication of secure material. It was concluded, on the other hand, that secure operation by either the REPLICA or AUTODIN II systems is possible and though difficulties were seen with both approaches in a review by NSA, there were indeed fixes that would make them usable at higher security levels.

- Security considerations are complicated by several factors but secure operation by either system is possible.
  - NSA role and approach constitutes a problem.
  - Implications of NSA's review are substantial.
  - Best approach is probably to meet NSA's security standards.
  - With NSA modifications, we believe either system is well protected.
  - Operational considerations favor WIN/ARPANET.
  - BLACKER development is essential to achieving multi-level security.

NSA Role

The peculiar role given to NSA in the process of security certification constitutes a real problem. Security always comes at the expense of an ability to function. Security procedures must be hammered out in the presence of the obvious conflicts that occur. In this case, NSA is in the position of rendering security judgments without having functional responsibilities for the working of the network or, in most cases, requirements of their own for the communication of the data involved. NSA has been given the role of being the watch dog of security and does so with a single minded commitment to identifying any risks that might occur when the system is put on line. Moreover, NSA's judgments are extraordinarily difficult to make because they require that the agency prove the negative: prove, in other words, that a threat to the system does not in fact exist. To do this requires that they anticipate devious workings the nature of which is really unknown within very complicated systems.

There appears to be an expectation that those with operational responsibilities will then make a balanced decision about the certification of the systems for use with classified data. It's not at all clear that these expectations are realistic. It is extraordinarily difficult for the operational authority to make decisions to use a system in the face of NSA concerns about security risks. What is lacking in this situation is the balanced assessment of security risks versus operational needs that is essential if such complex systems as these are ever to come on line. To some extent, security is never absolute; it is always relative and the question must be asked whether in existing circumstances we are operating with better security than we would be by adopting a new system. Since NSA does not have operational responsibility for systems such as DDN, it would be inappropriate for it to make the broader, balanced decision relating to operational certification.

Implication of NSA's Role

The implications of NSA's review of both the ARPANET and AUTODIN II systems were substantial. Interoperability, costs and program timing were all affected by the concerns that NSA had and their proposed fixes to meeting them. It appeared to us that the review put rather heavy reliance on traditional security standards as a basis for approval which frequently had, at most, a limited relationship to real system security. Despite these concerns, the Task Force concluded that the most expeditious approach is probably to accept NSA's recommendation for improving the security architecture of whichever system is chosen; but to work in the future toward a more balanced assessment of security requirements. To follow this course would require that additional IPLI's be added to both systems, the possible rewriting of some software using cleared personnel in a cleared facility, and that steps be taken to control hardware production to prevent the malicious modification of system elements during the production process. None of these is easy to accomplish or certain in effect, although they undoubtedly add to the cost of the program. With these NSA proposed modifications, however, the two approaches in our judgments are at least adequately armored to meet the security threats they are apt to encounter.

Operational Considerations

Several operational considerations on the other hand seem to favor the WIN/ARPANET approach. These have been mentioned above. Difficulties with the kernel particularly in terms of making modifications, making internal measurements and the needs for recertification become important considerations. Moreover, the substantially larger amount of software in the AUTODIN II kernel-based switch, some 150,000 lines of source code as compared with 15,000 lines of object code in the ARPANET switch, make it a substantially larger problem to maintain the AUTODIN II software. Though additional software is required with the addition of IPLI's to provide end-to-end encryption, it appeared to the Task Force that in order to get full security certification up to the S1 and ESI levels, IPLI's were going to be required on both systems. Thus, our conclusion was that in terms of the security considerations involved, our assessment had to favor the ARPANET/WIN approach over
AUTODIN II.

Costs

The Task Force addressed the question of costs with some skepticism. As noted above, component costs had been provided in part by contractors supporting the two design teams. Total estimated design team costs were then adjusted and normalized for comparsion by the evaluation team. These cost estimates gave a heavy edge to REPLICA. Nevertheless, there was so heavy a promissory ingredient in the proposal costs that the Task Force did not feel that they could be given much validity in absolute terms. Some fairly clear indicators did seem to emerge from the evaluation performed by DCA, however. The Task Force ultimately concluded that the costs as they were currently defined were uncertain, to say the least, but would probably favor the WIN/ARPANET approach.

- o Costs are currently uncertain but on a relative basis probably will favor ARPANET.
  - Will continue to be uncertain, particularly in the absence of firm contractor proposals.
  - In any event, up-front costs are a big problem, to avoid them by sticking with current program means significantly higher total costs.
  - Up-front costs mostly associated with providing Service to users expected to come on AUTODIN II and shouldn't be avoided for long.

Uncertainty

The principal factor undermining confidence in the costs as they had been generated was the fact that in both proposals significant inputs had been made by prime contractor supporting the design teams. As noted above, in neither case were they under any contractual obligation to actually perform as promised during the proposal preparation. As a result, there was a belief that though attempts were made to generate conservative costs, the uncertainties were very large and it was almost certain that cost growths would occur. This uncertainty is very much apt to continue until firm contractual arrangements are made with the contractors so that actual prices with commitments to meet them can be obtained.

Up-Front Costs of REPLICA Decision

However uncertain the costs may be, one thing is clear: there is a significant near-term cost problem if one adopts the WIN/ARPANET approach. This problem is caused by two considerations. One is the fairly substantial termination costs associated with ending the Westerm Union leasing arrangements for AUTODIN II and the other is a requirement to provide service for a number of users planning soon to join the AUTODIN II system. Projections of the tariff costs and access line costs by sticking with the AUTODIN II system ndicate that such a course would incur significantly higher total costs in the long run. In favoring a change to the WIN/ARPANET approach, the Task Force recognizes that OSD faces a difficult situation in trying to find the money to meet these near term requirements. It would be a great mistake to delay providing services to users expecting to come on AUTODIN II for any substantial length of time. In other words, an early solution to the up-front funding problem must be found if AUTODIN II is not continued.

User Satisfaction

User satisfaction and the ultimate achievement of a common user data communications network are extremely important goals that must not be overlooked. In a sense, they are what it is all about. If neither of these is achieved, the whole undertaking that was begun so many years ago makes little sense.

- o User satisfaction and development of a common user network are important goals.
  - Task Force approach favors creation of discrete nets accommodating user community peculiarities but maintaining a compatibility that will allow future consolidation.
  - A bottom-up rather than top-down approach.
  - Not all believe this approach is the best route to a common-user network, but all believe it's better than AUTODIN II.
  - Views about relative benefits of common user approach depend upon viewer's vantage point and must be considered.

Growth of Common User Network

The Task Force concluded that the best approach to the establishment of a common-user defense data network was the creation of discrete nets of users, accommodating user-community peculiarities, but maintaining a compatibility between nets that would allow for their future consolidation. This is a bottom-up rather than a top-down approach. Nevertheless, it takes into account some of the specific needs of various classes of users and tries to satisfy them as best it can and as early as possible. This approach then deals specifically with both sides of the problem: finding a means in which user satisfaction can be provided while at the same time working at a higher, broader level toward the ultimate achievement of a common user network. Not all members of the Task Force believed that this approach was the best route to take if one were starting afresh. There is a very natural concern that turning some users loose from a commitment to joining a common user network at the outset would make it impossible to recapture them at a later time. Others on the Task Force believed that the inclusion of users within discrete nets tailored to meet their needs and then the later incorporation of those nets into unified network would make this possible. In any event, all believe that the likelihood of achieving a common user network in the long run was higher with the ARPANET technology and this bottom-up approach than it would be with continuing AUTODIN II and trying to bring disappointed users aboard that system.

Differing Views about Common User Networks

Views about the relative benefits of common user systems depend upon the viewer's vantage point and this must be taken into consideration. Clearly there are some significant advantages of a common user network: interoperability, survivability, peakload capacity, reliability, costs, etc. But it is also true that these are more attractive to some users than to others. For the most part, they are attractive to the higher priority, high classification users who get most of the advantages of those capabilities that are built into the system. On the other hand, the lower priority, unclassified users must pay relatively more for the service that they get on the common user network. No really convincing set of comparative costs for the common user networks and dedicated links was at hand. Some had been prepared looking at the comparative costs for users who had dedicated links but were about to join AUTODIN II. These cost estimates were indeed frightening, at least from the user vantage point, but they may be suspect and indeed these cost estimates were contentious. But it remains true that the advantages of the common user network are unevenly shared. The higher the management level, the higher the priority and importance of the user, the better deal you get. For that reason, it is extremely important that OSD and DCA pay close attention to the process through which a common user network can be achieved. They must be the principal spokesmen for the advantages of such a system and it will be up to them to see that it is ultimately achievable. In performing that function, they must take into account the perceptions of the individual user and his own problem.

IV. TASK FORCE CONCERNS

Thus, the Task Force's own evaluation of the alternative plans for a defense data network led it to favor the adoption of the WIN/ARPANET approach. This conclusion was accompanied, however, with some major concerns.

- o We have some heavy concerns
  - Program management, configuration control and strategy
  - Security safeguard development
  - Host interfacing
  - Costs
  - User requirements data base
  - User treatment and system acceptance

Management

If a common user network is to be achieved, program management must really make it happen. The approach that we have proposed, a bottom-up rather than a top-down approach, puts a very heavy burden on management in this regard. It must maintain tight configuration control and insure the compatibility of the various networks that are established. It must see that necessary networks are formed to provide communities of users with common requirements and interests. Unless this is done, the likelihood of being able to co-opt all appropriate users is low. To accomplish all this requires that OSD and DCA develop a real strategy that will get computer communications from where it is today to a full common user network operating at multi-level security and including a broad range of users with substantially different requirements and needs. This strategy must also take into account the ways in which necessary funding will be obtained and management approaches that will insure some degree of stability and continuity in the way the program runs. There are sure to be tough times ahead, and confidence in the approach and in the system adopted must be maintained to get through them.

Development Risks

The WIN/ARPANET approach depends very heavily on the development of a number of security safequard devices. These include the IPLI which provides end-to-end encryption for the data carried on the network and serves as a gateway between nets. In the long run, true multi-level security operation will require development of the BLACKER system as noted above. Until that occurs and until we develop trusted hosts that are capable of handling multi-level security, we will be forced to deal with various security levels on a one-by-one basis. This means that additional IPLI's will have to be provided for users that deal at several levels of security. BLACKER development will

allow the easy distribution and change of key materials so that a multi-level security approach will become truly viable. These security device developments are not straight forward affairs and pose technical risks, particularly in the case of BLACKER. Management will have to see that pressure is kept upon these development programs in order that they meet schedules and stay within cost guidelines.

Host Interfacing

Host interfacing is another problem about which we have some concerns. The WIN/ARPANET approach provides for three levels of host interfacing. The most desirable of these is to modify host software so as to allow it to use the broad range of functions that are embodied in the ARPANET system. This approach carries with it significant difficulties as every host has its own peculiarities and there may not be space for the addition of new software or the making of software changes, etc. Other approaches will solve the problem but tend to become expensive in terms of true interoperability. The matter of host interfacing will be a point at which overall system management and the common user are apt to clash most immediately and advantages to the user of sticking with a dedicated link will appear strongest. This problem must be handled carefully and with due consideration to users concerns, needs and costs.

Costs

Not surprisingly, the Task Force is concerned about future costs. In part, this concern derives from the way in which the comparative costs were for developed for the evaluation. But a number of other factors could substantially affect projected costs as well. These include the substantial amount of development work that must be done on the security devices as noted above, the changes to the security architecture that may be required in order to satisfy NSA concerns about systems security, the almost certain discovery that the URDB is substantially different than it was projected to be in the evaluation process, and continuing growth in trunk costs, etc. All such factors will effect the ultimate costs of the system.

URDB

It became clear to the Task Force that the user requirements data base is woefully inadequate. Until it has been improved and made far more reliable than it seems to be at the present time, there is going to be no real understanding as what user communities must be established. This is something that needs early attention if a new approach is taken to the data network problem.

User Satisfaction

Finally, we were left with concerns about user acceptability and the process by which users can be drawn into a genuinely broad-based common user network. We are strongly of the view that OSD, in particular, must champion the cause of a common user network and take whatever steps are necessary to make that come to pass. In part, this will involve wooing the users to get them to break away from the dedicated links on which they have been relying and not making the costs or the disruptions associated with abandoning them so high that they will resist doing so. This question deserves a lot of serious attention in the months ahead.

V. DEFENSE SCIENCE BOARD AUTODIN II TASK FORCE RECOMMENDATIONS

The following recommendations were made to USDR&E on March 12, 1982:

1. OSD should reaffirm the need for a common-user network.

2. Make a choice between AUTODIN II and the WIN/ARPANET approach promptly; our review favors the selection of WIN/ARPANET.

We doubt that the preservation of AUTODIN II will significantly further the achievement of a common user net. Moreover, we believe that a better technical foundation for a Defense Data Network (DDN) is available. Though there are some significant programmatic and management risks associated with relying on accretions to the ARPA net foundation, we believe that these involve the extent and pace of common user participation and not risks involved in achievement of a common user net.

The most immediate impact of terminating AUTODIN II will be felt by users operating at the Secret level who might have been served more quickly by that system than by additions to the ARPA net base. While the Users Requirements Data Base (URDB) does not include a large number of Secret users, it is unquestionably incomplete.

3. In pursuing the development of a DDN, follow a program of gradual expansion of the WIN/ARPANET-compatible base with an eye toward the ultimate interconnection of individual nets.

But, this can only be done through aggressive pursuit of a fully developed program for the establishment of a broad common user network by institutionalized management and if the accretive process occurs under stringent configuration control.

4. The solution to the multi-level security problem for an ARPANET system requires the development of new security safeguard devices like BLACKER. The IPLI is an interim solution that is suitable until multi-level secure hosts become available.

The current IPLI program should be strengthened and the development consortium of DCA, DARPA, and NSA replaced by a single program manager. BLACKER development should be given higher priority.

VI. EPILOGUE

During the first 6 months, the Defense Data Network (DDN) Program has proceeded toward implementation along the path outlined in the REPLICA Program Plan. The Program Management Office (PMO) has been organized and staffing now includes 44 of the required positions. The PMO has assumed responsibility for the WIN Communications Subsystem (WINCS), the ARPANET, and the MINET. PMO personnel have made numerous trips explaining the DDN Program and signing up prospective subscribers. Funding requirements and the approach in meeting them have been worked out. In FY 83, offsets for DDN (RDT&E and Procurement Appropriations) have been identified to the Services and reprogramming will be accomplished through Congressional action. In FY 84-85 the Services' TOAs were increased for DDN. Funding for the DDN operations (O&M Appropriations) will be accomplished through the CSIF billing procedures.

The following actions are underway:

WIN — The IMP hardware to replace the aging Honeywell equipment has been ordered and site surveys have begun. Installation is scheduled to begin as soon as the IMP hardware is available.

ARPANET — The reconfiguration of the REPLICA into a MILNET for operational users and an experimental network is in the final planning stages with a logical separation of the network planning for Mid-1983.

MINET — The contract for the Phase I/Stage I testbed has been finalized. Installation of the network in Europe is scheduled to begin with the final IMP to be installed by November 1983.

SACDIN — The IMP and Monitoring Center hardware has been ordered and SIP interface development has been initiated. Planned for installation of a SACDIN network is underway.

Management Engineering Plan

A first draft of the MEP has been prepared and reviewed.
A second draft is currently being reviewed within the PMO.
A final draft is scheduled to be released for Service/Agency review in November 82.

Access Control

Access control for dialing subscribers to the DDN, a capability which was not provided for in the REPLICA Program Plan, will be required. This capability is currently under contract and will require 2 years for full development. An interim approach is planned.

In addition, the PMO has initiated action on Billing by Usage, Network Modeling, and Subscriber Interfacing. Modeling for the WIN and the ARPANET split is scheduled to start in November 82. A subscriber interface guide is under preparation and is scheduled to be available in November 82. A subscriber interface specification has been distributed to the Services for comment. A final interface specification is scheduled to be available by January 1983.

On October 6 and 7, 1982, the AUTODIN II Task Force reviewed progress on the development of the Defense Data Network since the inception of that program as a replacement for AUTODIN II in April 1982. Much has been accomplished during the past six months. Appropriate efforts have been made to establish program management that extends to the entire process of achieving a common user network through the eventual interconnection of dedicated networks serving separate communications. Maintaining the necessary configuration control to allow this eventual consolidation is a high priority management objective. Necessary funding commitments are in the process of being made throughout the FYDP. Serious attention is being given to improving the Users Data Requirements Base. In general, the Task Force was impressed with the response of OSD, DCA, and particularly the Program Office to implementing the DDN decision.

The program now faces a milestone decision in the selection of the DDN security architecture. We have examined proposed security architecture alternatives and NSA's review of them. The approach favored by the DDN Program Office (Option 2.2) consists of separate classified and unclassified networks to be connected ultimately through switch-level gates allowing classified traffic to exploit routing through the unclassified network but denying unclassified users access to the classified network. Development of the switch-level gate is required, but poses low technical risk and does not constitute a critical path in program scheduling.

Of the alternatives described by the Program Office, Option 2.2 seems to best balance the requirements for operational security assurance with user needs, and with technical and programmatic issues. In that regard, the Task Force supports the choice of Option 2.2 as best suited for implementation of a survivable, common user network serving both classified and unclassified users.

NSA's initial review of the architectural choices found the selected option to carry very low security risk but the judgment was qualified by a need to reconsider possible losses resulting from traffic analysis and the level of trust that could be attributed to switch software. Additional questions were raised about connecting MINET in Europe with MILNET in the U.S. These qualifications make the confident choice of a preferred architecture difficult.

Concerns about the security certification process and the confusion over NSA's institutional role and an overall determination of security adequacy were noted in the Task Force review of the DDN decision in March 1982. Those concerns were heightened during this meeting. It is essential that the choice of security architecture be made soon and that the choice be based upon a balanced assessment of security risks in light of existing practices, other sorts of risks, the relative likelihood of their occurring, and other threats to system reliability that might be introduced by corrective actions taken to eliminate low level computer security risks. It is likely, for example, that rewriting the heavily tested ARPANET switch code to meet NSA standards of trust would result in so great a loss of network stability as to make the possibility of the denial of service through an existing trap door in the present software a relatively minor concern. More will be said about this general problem below.

In order to aid decisionmaking on security architecture, it is recommended that NSA systematically decompose the findings of its review so as to organize its recommendations on the basis of the nature of the problem with which they deal; that is, identify those that are intended to prevent exposure or loss of data, those preventing hostile traffic analysis, and those defending against malicious denial of service. In the latter case, the source of malicious action should be identified, e.g., outsiders, unclassified users, or classified users operating against more highly classified portions of the network. Such a breakdown is made necessary by the fact that none of NSA's expressed concern about the preferred architecture relates to the actual loss of classified information and only an understanding of specific risks will make possible a broader assessment of the comparative risks involved and their larger significance.

There is, however, a larger problem associated with such assessments that will continue to plague not only this program but all future programs in the information systems area that pose security problems in new forms. Technology is outpacing even advanced thinking about computer and communications security. Moreover, the difficulties of conclusively establishing the non-existence of hazards, only a part of which we can expect even to imagine, have grown substantially with system complexity and size. NSA is left to deal with all this. The Agency endeavors to ferret out vulnerabilities that might be exploited by a skilled and well endowed adversary committed to doing so. This is an appropriate job for NSA and one that must be done. It does represent a singleminded look at the problem, however, one biased for understandable reasons toward dealing with all conceivable threats to security. It cannot by itself represent the entire assessment associated with the certification process.

There must be an additional step to explicitly take into account NSA's concerns as well as the security being provided by current communications systems and practices, the reliability with which they operate now and can be expected to operate under crisis conditions, the implications of security losses in varying circumstances, etc.

The Task Force believes that the NSA review tends to dominate this process unduly. In part, this is because of the professional competence and authority with which it addresses the security problem but also because it represents the safest position to adopt; it's hard to vote against security. We would urge that DUSD (C^3I) develop a set of explicit guidelines for making a broader assessment of security as a basis for certification and employ it during the DDN development and implementation process.

After hearing a discussion of the comparative survivability of various architectures, the Task Force urges that serious attention be given in this formative stage to taking all reasonable precaution by locating switches and other key network elements so as to improve physical survivability, and minimize intercept possibilities especially with regard both to the MILNET and Experimental-Net process of the ARPA net. Some important opportunities in this regard seem to exist. DUSD (C^3I) should follow this aspect closely and the DDN Program Office should strengthen its analytical efforts and make appropriate recommendations as to siting of network assests to enhance survivability.

THE UNDER SECRETARY OF DEFENSE

WASHINGTON, D.C. 20301

RESEARCH AND ENGINEERING

21 SEP 1981

MEMORANDUM FOR THE CHAIRMAN, DEFENSE SCIENCE BOARD

SUBJECT: Defense Science Board Task Force on AUTODIN II

You are requested to organize and convene a Defense Science Board (DSB) Task Force to review, evaluate and make recommendations concerning the continuation/termination of Defense Communications Agency (DCA) AUTODIN II data communications system.

BACKGROUND

AUTODIN II is the DCA common user data communications system under development since 1977 as a leased service from Western Union. The system met limited Initial Operational Capability (IOC) requirements on 5 July 1981. There are major questions about the survivability, security and cost of this critical system. Survivability is a serious concern because of the limited number of nodes and lack of expandability (at present there are only four packet switches for all of CONUS). NSA has expressed concerns about the HUMINT security of the system since it will operate with unclassified through intelligence community and SIOP data in the clear within each switch. Serious cost concerns have been expressed by the Defense Audit Service and the Air Force.

AUTODIN II is intended to provide the DoD with worldwide multilevel secure data communications services for critical command, control and intelligence functions and routine logistics and administrative functions. If the problems with AUTODIN II are sufficient to warrant its cancellation, the alternatives include existing packet switched networks such as the WWMCCS Intercomputer Network (WIN) and the ARPA network and planned capabilities such as the Movement Information Network (MINET).

The DSB Task Force should address questions of survivability, cost and security as applied to the AUTODIN II system and the presently available alternatives taking into account reasonable enhancements/upgrades to both capabilities. The Task Force should review the ongoing evaluation of both alternatives currently being conducted by DCA.

The Task Force should begin its work as soon as possible and should deliver a final report not later than 15 February 1982. Interim reports should be submitted as issues are resolved to the satisfaction of the membership.

This Task Force will be sponsored by Donald C. Latham, Deputy Under Secretary of Defense (C^3I). Mr. Stephen T. Walker, Director, Information Systems (ODUSD (C^3I)) will be the Executive Secretary.

APPENDIX B

MEMBERSHIP

DSB Task Force on AUTODIN II

Chairman

Dr. Sayre Stevens
Systems Planning Corporation

Members

Major General Van Doubleday, USAF (Ret.)
Honeywell Information Systems Inc.

Professor Seymour Goodman
University of Arizona

Mr. Gerald J. Popek
University of California

Dr. Harold Rosenbaum
Rosenbaum Associates, Inc.

Mr. John P. Stenbit
TRW, Inc.

Mr. Willis Ware
The RAND Corporation

Executive Secretary

Mr. Stephen T. Walker
Director, Information Systems, ODUSDRE/C^3I

DSB Secretariat Representative

Dr. Ralph E. Chatham, LCDR, USN
DSB Military Assistant

THE DEPUTY SECRETARY OF DEFENSE

APPENDIX C

WASHINGTON, D.C. 20301

2 APR 1982

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN, JOINT CHIEFS OF STAFF
DIRECTOR, DEFENSE COMMUNICATIONS AGENCY
DIRECTOR, DEFENSE INTELLIGENCE AGENCY
DIRECTOR, NATIONAL SECURITY AGENCY

SUBJECT: AUTODIN II Termination

In accordance with the unanimous recommendation of the Director, DCA, the Chairman of the Defense Science Board AUTODIN II Task Force and the Under Secretary of Defense for Research and Engineering, the Director of DCA is directed to terminate the AUTODIN II program as quickly as possible and to proceed immediately with the development of the Defense Data Network as outlined in the January 1982 ARPAnet Replica Program Plan. Programmatic and financial implications of this decision should be addressed in the FY 84 Program Objective Memorandum. It remains DoD policy that all data communications users will be integrated into this common user network. Exceptions to this policy must continue to receive the approval of the Deputy Under Secretary of Defense for C^3I.

Frank C. Carlucci

APPENDIX D

THE UNDER SECRETARY OF DEFENSE

WASHINGTON, D.C. 20301

RESEARCH AND
ENGINEERING

1 MAR 1982

MEMORANDUM FOR CHAIRMAN, DEFENSE SCIENCE BOARD

SUBJECT: Defense Science Board Task Force on the Defense Data Network

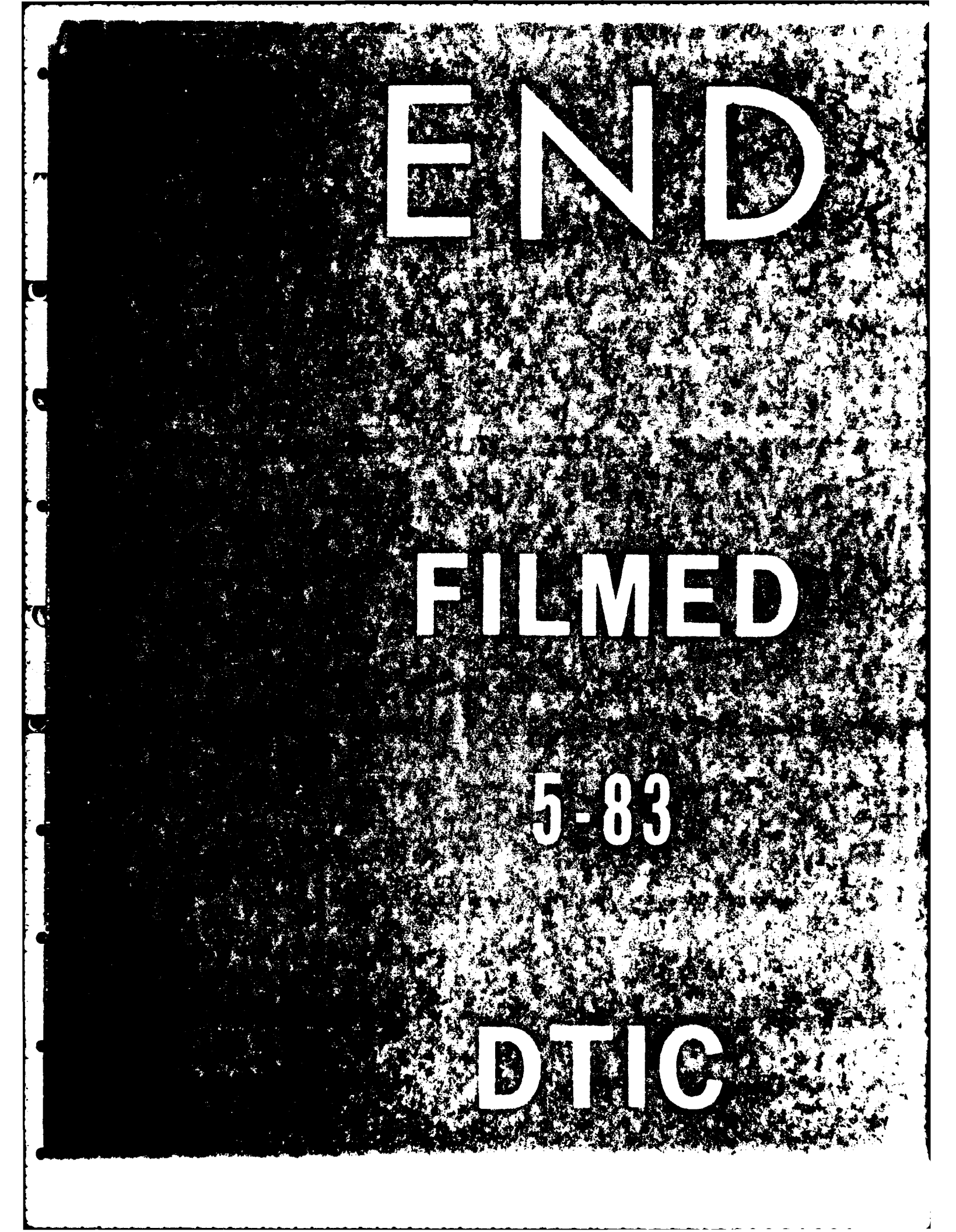
You are requested to organize and convene a Defense Science Board (DSB) Task Force to review, evaluate and make recommendations concerning the continuing evolution of the Defense Data Network (DDN) Program.

The DDN is the Defense-wide common user data communications system which resulted from the decision in April 1982 to terminate the AUTODIN II Program and provide data communications services to the Department through the evolution of existing ARPA network technology systems (e.g., ARPAnet, WWMCCS Intercomputer Network, Movement Information Network). Because of the critical nature of this project in providing the link between all DoD information systems, from highly sensitive C^3I systems to routine administrative and personnel systems, this program requires the extraordinary technical and management review which can only be afforded by a DSB Task Force.

The Task Force should address the full range of questions of network technology as applied to the DDN, cost, security, protocols, and other relevant topics.

The Task Force should begin its work as soon as possible. It should meet at least semiannually with the Senior Service Communicators and appropriate representatives of the JCS and Defense Agencies. A final report should be issued by October 1984 addressing these issues with a specific recommendation on the need for further review. Interim reports should be submitted as issues are resolved to the satisfaction of the membership.

This Task Force is sponsored by Donald C. Latham, Deputy Under Secretary of Defense (C^3I). Dr. Sayre Stevens, Chairman of the AUTODIN II Task Force, has agreed to serve as Chairman of this Task Force. Mr. Stephen T. Walker, Director, Information Systems (ODUSD (C^3I)), will be Executive Secretary. Dr. Ralph Chatham, LCDR, USN, will serve as DSB Staff Representative.


END
FILMED
5-83
DTIC